NASA Procedural Requirements

NPR NSS.1

Effective Date: XXXXX XX, XXXX
Expiration Date: XXXXXX XX, XXXX
Responsible Office: OSPP/Office of Security and Program Protection

---

National Security Systems

Table of Contents

Preface

P.1 Purpose

This NASA Procedures and Requirements (NPR) implements the National Security Systems (NSS) provisions of NASA Policy Directive (NPD) 2810.1C, NASA Information Security Policy. The NPR describes the NASA National Security Systems (NSS) Security Program, providing direction to ensure the protection of Classified National Security Information (CNSI) through the application of systems, equipment, technology, methodology, policies, and procedures designed to ensure confidentiality, availability, integrity, authenticity, and non-repudiation of CNSI in support of NASA.

P.2 Applicability

This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities. This NPR applies to JPL, or to other contractors, or grant recipients only to the extent specified or referenced in the appropriate contracts, grants, or agreements. NASA employees, NASA contractors, and NASA grantees to the extent in their contract or grant shall abide by these requirements when they perform work-related Agency missions, programs, projects, and institutional requirements involving NSS. Facilities, resources, and personnel under a contract or grant from NASA at a college, university, or research establishment are included in the applicability of this document. Address comments regarding this NPR to the Office of Security and Program Protection, NASA Headquarters, Washington, DC, 20546. Refer questions concerning the application of these requirements to specific NASA Centers to the appropriate NASA Center Security Office.

P.3 Authority

a. 42 U.S.C., Section 2473(c)(1), National Space Program.
b. Presidential Decision Directive (PDD) 49, National Space Policy.
c. Federal Information Security Management Act of 2002.
d. Presidential Decision Directive (PDD) No. 63, Subject: Critical Infrastructure Protection, dated 22 May 1998
e. Executive Order 12958, Classified National Security Information, as amended (March 2003).
f. 32 CFR, Part 2001, ISOO Directive No.1.
g. Index of National Security Telecommunications Information Systems Security Issuances (NSTISSI).
h. NSTISSI 4003, Reporting and Evaluating COMSEC Incidents.
i. National Security Directive 42, National Policy for the Security of National Telecommunications and Information Systems.
j. 44 U.S.C. 3501 et seq., the Paperwork Reduction Act of 1995, as amended.
k. 40 U.S.C. 1401 et seq., the Clinger-Cohen Act of 1996, as amended.
l. 44 U.S.C. 1441 et seq., the Computer Security Act of 1987, as amended.
m. 5 U.S.C. App., the Inspector General Act of 1978, as amended.
n. 5 U.S.C. 552a, the Privacy Act of 1974, as amended.

o. 18 U.S.C. 2510 et seq., the Electronic Communications Privacy Act of 1986, as amended.
p. Executive Order 13011, Federal Information Technology.
q. Executive Order 12333, United States Intelligence Activities
r. Director, Central Intelligence Directive 6/3 (DCID 6/3)
s. NPD 2810.1C, NASA Information Security Policy
t. NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products
u. NSTISSP No. 12, National Information Assurance (IA) Policy for U.S. Space Systems
v. NSTISSI No. 4005, as amended, Safeguarding Communications Security (COMSEC) Facilities and Materials
w. NSTISSI No. 4003, Reporting and Evaluating COMSFC Incidents
x. National Industrial Security Program Operating Manual (NISPOM) Supplement Overprint
y. CNSS Instruction 4009, National Information Assurance Glossary
z. NIST Special Publication 800-59, Guidelines for Identifying an Information System as a National Security System

P.4 References

a. 14 CFR, Section 1203, National Aeronautics and Space Administration.
b. NPR 1600.1, NASA Security Program Procedural Requirements.
c. NPR 1600.2, Physical Security Vulnerability Risk Assessments
d. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property
e. NPD 1382.17E, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulations.
f. NPD 1440.6G, NASA Records Management.
g. NPD 1600.2C, NASA Security Policy.
h. NPD 2800.1A, Managing Information Technology.
i. NPD 7120.4, Program/Project Management.
j. NPD 9800.1, NASA Office of Inspector General Programs.
k. NPR 1441.1D, NASA Records Retention Schedules.
l. NPR 7120.5, Program and Project Management Processes and Requirements.
m. Executive Order 13231, Critical Infrastructure Protection in the Information Age
n. Executive Order 13284, Executive Order Amendment of Executive Orders and Other Actions
o. NSTISSI 1000, National Information Assurance Certification and Accreditation Process (NIACAP)
p. NSTISSI 4012, Senior System Managers
q. NSTISSI 4013, System Administrator
r. NSTISSI No. 4015, National Training Standard for System Certifiers
s. CNSS 4014, Information Systems Security Officer (ISSO).
t. Defense Information Technology Security Certification and Accreditation Process Implementation Manual

u. NSA Manual 130-2, Media Declassification and Destruction
v. NPD 4200.1A, Equipment Management
w. Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems

P.5 Cancellation

None

/S/
David A. Saleeba
Assistant Administrator
Office of Security and Program Protection

CHAPTER 1: General

1.1 Responsibilities

1.1.1. The Assistant Administrator, Office of Security and Program Protection shall:

a. Provide overall policy direction and procedural requirements for NASA National Security Systems (NSS) assets by issuing policies, directives, instructions, and advisory memoranda.
b. Coordinate with Institutional Program Offices (IPO) and Center Directors, as necessary, to ensure appropriate application of established NSS policy, procedures, and requirements pertaining to the protection of NASA NSS assets.
c. Serve as the Principle Accreditation Authority (PAA) for the certification and accreditation of NASA's National Security Systems.

1.1.2. Center Directors shall:

a. Ensure Center security personnel conduct the appropriate threat, risk, and vulnerability assessments for all NSS assets under their control in a timely manner under the auspices of the OSPP.
b. Ensure senior management officials at their respective Center implement physical security measures commensurate with the requirements established in this NPR.

1.1.3. Center Chiefs of Security shall:

a. Ensure a physical security vulnerability risk assessment is conducted for all NSS assets under their control in a timely manner. At a minimum, all Minimum Essential Infrastructure (MEI) assets, as defined in NPR 1600.1, NASA Security Program Procedural Requirements, shall be subject to the appropriate security vulnerability risk assessment immediately upon designation as critical infrastructure and/or key resource, particularly with regards to NSS.
b. Ensure the physical security measures identified in this NPR and other national and NASA policies are implemented.
c. As appropriate and required, notify the NASA Office of Inspector General of all crimes at NASA owned and/or leased facilities, to include theft or misuse of, or damage to Government property.

1.1.4. Organizational Heads shall control and safeguard all national security information and NSS assets within their activity. They shall:

a. Promptly report to the Center law enforcement/security organization, and assist in any investigative activity and resolve incidents involving loss, theft, misuse, or damage of NASA NSS resources.

b. Establish and document end-of-day security checks (e.g., Standard Form (SF) 701 Activity Security Checklist) when storing classified material or equipment (e.g., hardware, software, firmware, or storage media).
c. Implement physical security measures commensurate with the results of threat, risk, and vulnerability assessments in order to adequately protect NSS.

1.2 National Security Information and National Security Systems Overview

1.2.1. National Security Information (NSI), often referred to as classified NSI (CNSI) and is information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure.

1.2.2. A National Security System (NSS) is any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

a. involves intelligence activities;
b. involves cryptologic activities related to national security;
c. involves command and control of military forces;
d. involves equipment that is an integral part of a weapon or weapon system; or
e. is critical to the direct fulfillment of military or intelligence missions and does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);
f. is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

1.2.3. There are three basic categories of NSI processed by a NSS.

a. *Collateral*: The current classification system of NSI consists of three levels of classification (Confidential, Secret, and Top Secret), which is often referred to collectively as Collateral.
b. *Sensitive Compartment Information (SCI)*: SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems that are established by the Director of National Intelligence.
c. *Special Access Program (SAP)*: A SAP is a security program established under the provisions of Executive Order (EO) 12958 as amended and approved by the Departments of Defense or Energy to apply extraordinary security measures to protect extremely sensitive information. The level of controls is based on the criticality of the program and the assessed hostile intelligence threat.

1.2.3.1. The DoD Overprint to the National Industrial Security Program Operating Manual Supplement (NISPOMSUP) recognizes three categories (sub-categories) of SAPs: acquisition, intelligence, and operations and support.

a. *Acquisition SAPs* protect sensitive research, development, testing, modification, and evaluation or procurement activities in support of sensitive military and intelligence requirements.
b. *Intelligence SAPs* protect the planning and execution of especially sensitive intelligence or Counterintelligence (CI) units or operations, including the collection, analysis, and exploitation of intelligence. Intelligence SAPs also protect especially sensitive programs to procure and exploit foreign materiel.
c. *Operations and support SAPs* protect the planning, execution, and support to especially sensitive military operations. This type of SAP may protect organizations, property, operational concepts, plans, or activities.

1.2.3.2. There are two types of SAPs, *Acknowledged* and *Unacknowledged*.

a. An *Acknowledged SAP* may be openly recognized or known; however, specifics within the SAP will be classified.
b. The existence of an *Unacknowledged SAP* or an unacknowledged portion of an *Acknowledged* SAP will be made known only to those personnel properly authorized to receive the information.

1.2.3.3. The levels of SAP protection are as follows:

a. *Waived SAP*;
b. *Unacknowledged SAP*;
c. *Acknowledged SAP*.

1.3 Terms and Definitions

1.3.1. Communications Security (COMSEC)

a. *COMSEC* is the measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. The National Security Agency (NSA) is the executive agent for developing and implementing national level policy affecting the control of COMSEC material. NSA is also responsible for the production and distribution of most COMSEC material used to secure communications as well as the development and production of cryptographic equipment.
b. *Cryptosecurity* is a component of COMSEC resulting from the provision of technically sound cryptosystems and their proper use.

c. *Transmission security (TRANSEC)* is a component of COMSEC resulting from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

d. *Emission* security is the protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an information system.

1.3.2. Information Systems Security (INFOSEC)

a. *INFOSEC* is the protection of information systems (IS) against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

1.3.3. Information Assurance (IA)

a. Information assurance (IA) is the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

1) *Availability*. Timely, reliable access to data and information services for authorized users.

2) *Integrity*. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

3) *Authentication.* Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

4) *Confidentiality*. Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

5) *Non-repudiation*. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

1.3.4. TEMPEST is the short name referring to investigation, study, and control of compromising emanations from IS equipment.

1.3.5. Other terms and definitions may be found in CNSS Instruction 4009, National Information Assurance Glossary

1.4 NSS Policies and Sources

1.4.1. *Collateral*

a. Under Executive Order (E.O.) 13231 of October 16, 2001, Critical Infrastructure Protection in the Information Age, the President re-designated the National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS). The Department of Defense chairs the Committee under the authorities established by NSD-42. This was reaffirmed by Executive Order 13284, dated January 23, 2003, Executive Order Amendment of Executive Orders and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security.

b. The CNSS provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems. The CNSS, the Subcommittee on Telecommunications Security (STS), the Subcommittee on Information Systems Security (SISS), and their joint working groups serve as the primary source for policy for *collateral* national security systems, COMSEC, INFOSEC, TRANSEC, and TEMPEST. They are published in the Index of National Security Systems Issuances containing policies, directives, instructions, and advisory memoranda.

1.4.2. *Sensitive Compartmented Information (SCI).* NSS that process SCI must be in compliance with Director of Central Intelligence Directives (DCID's), which is under the Director of National Intelligence.

1.4.3. NSS that are affiliated with *Special Access Programs* must be in compliance with the DoD Overprint to the National Industrial Security Program Operating Manual Supplement (NISPOMSUP) and applicable DCID's depending on the type of SAP.

CHAPTER 2: National Security Systems (NSS)

2.1 General

2.1.1. All NASA-managed (owned or controlled) national security systems (NSS), and the components thereof, that collect, generate, process, store, display, transmit, or receive national security information, as defined by E.O. 12958 as amended and by Act or Law of Congress, shall be in appropriate compliance with national policies implemented by Executive Orders, Presidential Decision Directive(s), laws, regulations, policies prescribed by the Committee on National Security Systems (CNSS), Director of Central Intelligence Directives corresponding to SCI, and defined SAP policy and guidelines. Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333. Although NIST Special Publication 800-59, Guidelines for Identifying an Information System as a National Security System, specifies that national security systems are not required to follow NIST standards, NASA national security systems shall meet the minimum equivalent security objectives set forth for a “High” Potential Impact IS identified in FIPS Publication 199 as described in NPR 2810.1. National security policy and guidance shall take precedence where there is conflict or uncertainty.

2.2 Information Assurance

2.2.1. Information Assurance (IA) shall be factored into the entire lifecycle for a NSS, to include planning, requirements generation, initiation, research, budgeting, development, acquisition, testing, evaluation, production, deployment, implementation, operation, maintenance, education, training, and disposal.

2.3 Acquisition Planning

2.3.1. Technological advances and threats of the past decade have drastically changed the way we think about the products that we acquire for protecting our communications and communications systems. A CNSS policy, NSTISSP 11, has been developed as a means of addressing commercial security and security-enabled IA products as alternatives to traditional government-off-the-shelf products. Commercial-off-the-shelf IA or IA-enabled IT products (i.e., hardware, software, and firmware) being considered for use in NSS shall be limited to products that have been evaluated and validated in accordance with the requirements of NSTISSP No.11 by the National Institute of Standards and Technology (NIST) or in accordance with processes approved by NSA. Exceptions will be considered in accordance with NSTISSP 11, Annex A.

2.4 Certification and Accreditation

2.4.1. Communications and information systems (e.g., NSS) that process Classified National Security Information (CNSI) shall be certified and accredited (C&A) for the level of information (e.g., Confidential (C), Secret (S) , or Top Secret (TS)) that it will be processing prior to allowing that system to become operational. NASA shall complete a checklist as defined in NIST Special Publication 800-59, Guidelines for Identifying an Information System as a National Security System, to determine if a system is considered to be a NSS. The checklist shall be maintained as part of the certification and accreditation documentation. Dependant on the level (e.g., C, S, or TS) and type of information (e.g., *collateral*, *SCI*, or *SAP*) that is to be processed, viewed, stored or manipulated; a determination of the requirements must be made. After the determination of requirements, each individual NSS shall follow the appropriate set of policies and standards for physical, personnel, information, transmission, and communications security to include TEMPEST. Each NSS shall be certified and accredited (C&A) as follows:

a. *Collateral* NSS shall follow National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, National Information Assurance Certification and Accreditation Policy (NIACAP) for C&A. The Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Implementation manual shall be used as a tool for the NIACAP until the CNSS publishes a CNSS/NIACAP Implementation Manual (or equivalent).

b. *SCI* NSS shall be in compliance with the DCID's and follow DCID 6/3 for C&A.

c. *SAP* NSS shall follow the specified SAP Security Policy and shall meet C&A guidelines (e.g., NIACAP or DCID).

Contact the NASA HQS OSSP, Systems Security Manager, at 256-544-3856 for the most current System Security Authorization Agreement (SSAA) and Systems Security Plan formats.

2.4.2. All NASA National Security Systems shall be certified and accredited to support the overall end-to-end security of the system regardless of the type of information (e.g., *collateral*, *SCI*, or *SAP*). Access to classified NSS must be restricted to properly cleared individuals whose official duties require access to NSS. The fact that an individual has a security clearance and/or holds a certain rank or position, does not, in itself, entitle an individual access to NSS. Access to classified as well as unclassified systems / material requires a valid need-to-know.

2.4.3. National Security Systems that reside on NASA owned, leased, or managed property that belong to outside agencies, organizations, or entities shall be certified and accredited. They shall also be coordinated and approved in writing by NASA HQS OSPP prior to their operation with no exceptions.

2.5 NSS Functions and Responsibilities

2.5.1. In order to insure proper and timely application of this guidance, roles and responsibilities within the agency must be established and defined. For this purpose, this guidance serves as the official establishment of these roles and defines the responsibility of each.

2.5.2. *Principle Accrediting Authority (PAA)*: The Principle Accrediting Authority (PAA) is the senior NASA official having the authority and responsibility for all national security systems within NASA. The PAA is the Assistant Administrator, Office of Security and Program Protection (OSPP). The NASA PAA may delegate responsibilities to other OSPP individuals (e.g., OSPP, Director of Security Management Division), but shall be done by appointment letter and the NASA PAA retains ultimate responsibility. The responsibilities of the PAA include but are not limited to:

a. Establishing and maintaining NASA's NSS program(s), including certification and accreditation programs and processes.
b. Ensuring the formal written appointment of Designated Approval Authority's (DAA's) for each NASA NSS and the appropriate categories of CNSI (e.g., *collateral*, *SCI*, or *SAP*). The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.
c. Exercising top-level management oversight of the development, implementation, and evaluation of NSS programs.
d. Ensuring the establishment of a NSS incident response and reporting capability, which shall include all categories of CNSI (e.g., *collateral*, *SCI*, or *SAP*).
e. Ensuring accountability for the protection of the information under the PAA's purview, including maintenance of required documents concerning the accreditation status of systems.
f. Establishing NSS security education, training, and awareness programs to ensure consistency and reciprocity.
g. Establishing a compliance validation and oversight mechanism to ensure consistent implementation of the security policy requirements set forth in this NPR.
h. Ensuring that security is incorporated into the entire NSS life-cycle process.
i. Serving as DAA for a NASA *collateral* or *SAP* NSS.
j. Ensuring NASA national security systems have appropriate budgets to prevent program managers from "cutting corners" on security to reallocate dollars to other aspects of the program; thereby, potentially jeopardizing national security.
k. Ensuring there is a duly appointed Certified TEMPEST Technical Authority (CTTA) for NASA national security systems and NSA TEMPEST requirements are met.
l. Ensuring NASA national security systems are inventoried and receive independent assessments to meet compliance with the FISMA.
m. Providing equipment management accountability for national security systems that may exempt from the NASA Equipment Management System (NEMS). See paragraph 2.10 for more information.

2.5.2.1. The NASA PAA may duly appoint a PAA Representative to assist him or her in the carrying out of the PAA duties.

2.5.3. *Designated Approving Authority (DAA)*: Each NASA NSS shall have a duly appointed Designated Approving Authority. The DAA is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with *designated accrediting authority* and *delegated accrediting authority* and *Senior Systems Manager* as defined by CNSSI 4012. Because of the possible confusion within NASA relating to the new term *Senior Systems Manager* for NSS and existing senior systems managers that serve in a technical, but non-security role, NASA will at this time continue to use the term DAA for NSS in lieu of *Senior Systems Manager*.

2.5.3.1. The DAA grants formal accreditation to operate an information system processing national security information. The DAA has the authority to withdraw accreditation, suspend operations, grant interim approval to operate, or grant variances when circumstances warrant. The approval shall be a written, dated statement of accreditation that clearly sets forth any conditions or restrictions to system operation.

2.5.3.2. The type of NSS (e.g., *collateral*, *SCI*, or *SAP*) will determine who shall serve as the DAA. The usage of the system may also be a deciding factor. Each NASA DAA is responsible for receiving training that has been recognized by the CNSS as meeting the standards in NSTISSI No. 4015 for the position held. The following information provides some insight on who may serve as DAA's for NASA NSS:

a. *Collateral* DAA's are generally NASA officials. However, there are circumstances where a NASA NSS may interconnect to another Agency's network (e.g., Secret Internet Protocol Router Network also referred to as SIPRNet). In this example, the Defense Information Systems Agency (DISA) serves as the overall DAA for SIPRNet. NASA may have local DAA's participate in the C&A documentation process involving a local Center

b. *SCI* DAA's are Intelligence Community (IC) officials (e.g., CIA, NSA, DIA, or NRO).
c. *SAP* DAA's may be a NASA official, IC official or other agency official depending on the program and interagency agreements.

2.5.3.3. The NASA PAA shall be responsible for determining who shall serve as the appropriate DAA for a NSS within NASA. NASA Centers and DAA's may request that a DAA Representative be appointed to assist in the carrying out of their responsibilities. The process for nominating a DAA Representative is the same as for a DAA and the individual must also meet the training standards established to be a DAA. The DAA retains ultimate responsibility for risk acceptance.

2.5.4. *Certifying Authority (CA)*: The Certifying Authority (CA) for a NSS is the individual responsible for managing the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements. The CA is responsible for all systems at their location or purview; this includes single system and multiple systems configurations. However, they must be identified in the system accreditation documentation as the CA for that system. If the system is a network that has connections at other NASA locations, there will be a principle CA for the network server location and each location with a connection, which will require having a CA for the system at their location. CA duties include making technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages. As a minimum, each designated CA is responsible for receiving training that has been recognized by the CNSS as meeting the standards in NSTISSI 4015 for the position held. The Systems Operation Manager, NASA HQ OSPP, has CA oversight responsibility for all *collateral* and *SCI* NSS within NASA.

2.5.5. *Information System Security Manager/Information System Security Officer (ISSM/ISSO)*: The Information System Security Manager/Information System Security Officer (ISSM/ISSO) serve as the official(s) responsible to the DAA for ensuring the security of an information system throughout its life cycle, from design through disposal. The ISSM is the principle government person in this position whereas a properly trained and appointed contractor may serve as an ISSO. The terms ISSM and ISSO are sometimes used interchangeably, or functions performed by the same individual. The Systems Security Manager, NASA HQ OSPP, has ISSM oversight responsibility for all NSS within NASA. The local ISSM/ISSO's may be responsible for a single system or multiple systems at their location. However, they must be identified in the system accreditation documentation as the ISSM/ISSO for that system. If the system is a network that has connections at other NASA locations, there will be a principle ISSM/ISSO for the network server location and each location with a connection will be required to have ISSM/ISSO for the system at their location. Each ISSM/ISSO is responsible for receiving training that has been recognized by the CNSS as meeting the standards in NSTISSI 4014 for the position held.

2.5.5.1. The ISSM is an individual responsible for NSS for an organization (e.g., Center). The responsibilities of the ISSM include but are not limited to:

a. Developing and maintaining a formal information technology security program for NSS.
b. Implementing and enforcing NSS policies.
c. Reviewing all system security plans (SSP's), system security authorization agreements, certification and accreditation packages, and endorsing those found to be acceptable.
d. Overseeing all ISSO’s under their direction to ensure that they are following established information security policies and procedures; ensuring that necessary technical and security training is available to carry out their duties.
e. Ensuring the development of system certification documentation by reviewing and endorsing such documentation and recommending action by the DAA.
f. Maintaining, as required by the DAA, a repository for all system certification documentation and modifications.
g. Coordinating information system security inspections, tests, and reviews.
h. Developing procedures for responding to security incidents, and for investigating and reporting (to the DAA) security violations and incidents, as appropriate.
i. Ensuring proper protection or corrective measures have been taken when an incident or vulnerability has been discovered within a system.
j. Ensuring development and implementation of an information security education, training, and awareness program.
k. Ensuring development and implementation of procedures for authorizing the use of software, hardware, and firmware on the system.

2.5.5.2. The ISSO is responsible to the ISSM for ensuring that operational security is maintained for a specific information system. The ISSO ensures systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the security plan. Specific responsibilities include but are not limited to:

a. Ensuring that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access to the IS.
b. Reporting all security-related incidents to the ISSM; coordinating with the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.
c. Developing and maintaining a system security plan (SSP) and certification and accreditation (C&A) packages.
d. Conducting periodic reviews to ensure compliance with the SSP's / C&A.
e. Ensuring configuration management (CM) for security-relevant system software, hardware, and firmware is maintained and documented.
f. Ensuring all security-related documentation is current and accessible to properly authorized individuals.
g. Formally notifying the ISSM and the DAA when a system no longer processes national security information.
h. Formally notifying the ISSM and the DAA when changes occur that might affect the security posture of the accreditation.
i. Ensuring that system security requirements are addressed during all phases of the system life cycle.
j. Following procedures developed by the ISSM, authorizing software, hardware, and firmware use before implementation on the system.

2.5.6. *Systems Administrator (SA)*: Individual responsible for the system installation and maintenance, providing effective information system utilization, adequate security parameters, and sound implementation of established IA policy and procedures. The SA may be responsible for a single system or multiple systems at their location; however, they must be identified in the system accreditation documentation as the SA for that system. Larger and more complex systems will require a dedicated SA to ensure that all requirements for system configuration and management are maintained. The SA is responsible for the day-to-day management of the system and users profiles. The SA is responsible for monitoring system performance, insuring current software patches and virus scan definitions are installed and operating properly, monitoring and enforcing security protocols, and reporting incidents and violations in a timely manner. If the system is a network that has connections at other NASA locations, there will be a principle SA for the network server location and each location with a connection will be required to have SA for the system at their location. Each SA is responsible for receiving training that has been recognized by the CNSS as meeting the standards of NSTISSI 4013 for the position held. The Systems Operation Manager, NASA HQ OSPS, has SA oversight responsibility for all NSS within NASA.

2.6 NSS Center Management Roles

2.6.1. Each NASA Center that has National Security Systems (NSS) assigned, operational and in development, are required to identify and establish a DAA, CA, ISSM/ISSO, and System Administrator for the system(s) located on that Center. The NASA Center DAA will be nominated by the Center Director and appointed by the NASA HQS PAA. Note: As stated previously, DAA's for NSS that process SCI are within the Intelligence Community (e.g., CIA, DIA, NSA, or NRO). Upon being appointed in writing, a NASA DAA is required to attend training that has been recognized by the Committee on National Security Systems (CNSS) as meeting the standards described in NSTISSI 4012 for the position held. The DAA is responsible for appointing or establishing a Certifying Authority, Information System Security Manager/Information System Security Officer, and System Administrator for each NASA system(s) at that location. Designated positions may be responsible for multiple systems, but are required to evaluate and support each system individually. A NASA Center may also have more than one DAA per Center, but shall be approved by the NASA PAA based on needs and requirements.

2.6.2. A NASA DAA is responsible for establishing a program for reporting incidents that occur at their location or under their purview as well as an annual inventory of their NSS, which shall be provided to NASA HQS OSPP. Prior to the development of a new NSS at their location, the NASA DAA will coordinate NSS requirements with the NASA HQ OSPP. Responsibilities of a NASA DAA include but are not limited to:

a. Overseeing the implementation of the security policy and providing guidance for securing NASA Systems.
b. Ensuring that security testing and evaluation are completed and documented.
c. Maintaining appropriate system accreditation documentation.
d. Evaluating risks, threats and vulnerabilities to ascertain whether additional safeguards are needed.
e. Ensuring that a record of all security-related vulnerabilities and incidents is maintained, and reporting serious or unresolved violations.
f. Ensuring that C&A is accomplished for each NSS under their purview.
g. Evaluating certification documentation and providing written recommendations for accreditation.
h. Ensuring that all ISSM's and ISSO's under their direction receive technical and security education and training to carry out their duties.
i. Assessing changes in the system, its environment, and operational needs that could affect the accreditation or re-accreditation.
j. Ensuring the impact of wireless devices, services, and technologies are appropriately addressed in Chapter 10 of this NPR.

2.7 NSS End User Roles

2.7.1. End Users of NSS are the key element in protecting and maintaining the integrity of national security. From ensuring that normal operation instructions are followed to reporting incidents, the user has day-to-day responsibility for protecting NSS.

2.7.2. End Users with access to NSS IT shall become familiar with the System Security Authorization Agreement (SSAA) or system security plan (SSP) applicable to that system and shall abide by the requirements of the SSAA or security plan.

2.7.3. End Users with access to COMSEC equipment and keying material shall be properly briefed by the local servicing COMSEC Account Manager (CAM). NSS users shall become familiar with NASA COMSEC Standard Operating Procedures (CSOPs) that apply to the COMSEC for which they have access. COMSEC is described in more detail later in this NPR.

2.7.4. A NSS End User is an individual who can receive information from, input information to, or modify information on, a NSS without a reliable human review. NSS End Users are responsible for:

a. Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assuming only those roles and privileges for which they are authorized.
b. Immediately reporting all security incidents and potential threats and vulnerabilities involving a NSS to the appropriate ISSO.
c. Ensuring that system media and system output are properly classified, marked, controlled, stored, transported, and destroyed.
d. Protecting terminals/workstations from unauthorized access.
e. Use the NSS only for authorized purposes.
f. Not introduce malicious code into any NSS or physically damage the system.
g. Not introduce or use unauthorized software, firmware, or hardware on a NSS.
h. Not relocate or change NSS equipment or the network connectivity of NSS equipment without proper security authorization.
i. Obtaining and following the NSS education, training, and awareness briefing(s) applicable for their particular system.
j. Complying with NSS user agreements for their particular system. In accordance with the training program requirements, each individual with access to national security systems shall be required to sign a National Security Systems User Agreement. This agreement will outline the individual's responsibilities and requirements for maintaining access to the system. The original signed copy of the agreement will be maintained by the applicable DAA.

2.8 Security Awareness, Education, and Training

2.8.1. The key elements for a successful security program are education, training, and awareness. These main elements provide a knowledge base concerning Classified National Security Information and the systems that protect it, whether processed, stored, transmitted, or archived.

2.8.2. The DAA at each NASA Center shall be required to implement a program of awareness, education, and training that covers the unique issues associated with NSS and COMSEC under their purview. The program shall include initial training prior to granting access to any NSS. In addition, yearly refresher training, quarterly educational reminders, as well as a method of keeping personnel aware of their responsibilities to secure and protect Classified National Security Information and systems must be strictly adhered to. Awareness can be accomplished through flyers, email reminders, posters, and others items that get the person's attention and reminds them of their role in security.

2.9 Incident Reporting and Handling

2.9.1. There are two distinct elements of NSS reporting that must be considered should a NSS incident occur. First, the determination must consider if COMSEC is potentially involved. If so, the procedures outlined in the COMSEC chapter of this NPR relating to COMSEC Incidents, shall be followed. The second element of consideration is to determine the type of NSS (e.g., collateral, SCI, or SAP), which will determine the specific handling requirements of the alleged incident.

2.9.2. To facilitate the reporting of NSS incidents, NASA HQ OSPP has established a NSS incident reporting process with the contractor provided NSS Support Team located at Marshall Space Flight Center. The team has established duty hours of 0600 – 1800 CST, Monday through Friday. The team can be reached at 256-544-4935 during normal duty hours. For after hours, weekends, and holidays, this number will rollover to the on-call cell phone and a member of the NSS support team will be available to provide assistance. A member of the team is available to the customer community 24 hours a day, 365 days a year. The support team can also be reach via unclassified email at **nss@msfc.nasa.gov** and via classified email at **contact@nsn.nasa.sgov.gov**. All questions and answers will remain UNCLASSIFIED for the initial notification. (Note: If classified information is required for a complete picture of the incident, contact information will be obtained and follow-up will be made by appropriate secure communications.)

2.9.3. Upon receipt of the incident notification, the NSS Team member will log the outage using an internal automated tracking system. The incident will be tracked to completion, archived for future reference and included in quarterly trend analysis numbers. The Systems Security and Operations Security Managers have access to the automated system employed by the team and can view incident information at any time. The NSS Team member will then pass the information to the Systems Security Manager, (256) 544-3856, NASA OSPP. Hard copy documents will be forwarded to MSFC/AS50, attention NASA HQ OSPP representative.

2.9.4. After evaluating the information provided, NASA HQ OSPP will determine, utilizing the Information Technology Sanitization and Cleanup (ITSC) Initial Reporting/Preliminary Administrative Inquiry Form, and User Interview and Incident Worksheet Form, the extent of the inquiry that is required and individuals to be involved. Incidents of a criminal intent nature will be referred to the NASA Office of Inspector General, while incidents of a counterintelligence nature will be referred to the NASA HQ OSPP, Safeguards Division. The Director, Security Management Division, in the OSPP will investigate incidents not falling into one of these two categories.

2.10 NASA Equipment Management System (NEMS)

2.10.1. The NASA Equipment Management System (NEMS) shall be used throughout the Agency to identify, control, and account for Government-owned equipment acquired by or in use by NASA, which includes equipment that processes national security information and meet the parameters established by NPD 4200.1A. The only exceptions are Communications Security (COMSEC) materials and equipment, which are addressed separately in this NPR (Chapter

8.2.3), and national security systems equipment deemed to be classified as having an Operations Security (OPSEC) impact. In such rare cases, only the NASA PAA may exempt such equipment from NEMS, which shall be documented and placed in the applicable SSAA/SSP and requires the NASA DAA/CA to implement equipment accountability equivalent or more stringent than NEMS. The tagging and tracking of national security systems equipment in the NEMS shall be done in such a way as to not to divulge the security characteristics of the system or national security information itself. OPSEC shall be factored in the accounting process and dictate the specifics. National security systems shall be appropriately sanitized prior to access for tagging and accounting requirements by NEMS personnel. Classified magnetic media or NSS output shall not be placed into the NEMS process.

CHAPTER 3: COMMON NSS REQUIREMENTS

3.1 Introduction.

This section describes the protection requirements that are common to all NSS.

3.2 Media Clearing and Sanitization.

3.2.1. Storage media shall be physically controlled and safeguarded in the manner prescribed for the most-sensitive designation, or highest classification level, and category of data ever recorded on it until destroyed or sanitized using approved procedures. The SSAA/SSP shall specify the approved release procedure for the media of a given system. Procedures to be used for the sanitization, declassification, and reuse of storage media are described below:

a. *Clearing* is the process of eradicating the data on the media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval.
b. *Purging* or *sanitizing* is the process of removing the data from the media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before purging or sanitizing. In general, laboratory techniques cannot retrieve data that has been purged or sanitized.
c. *Destroying* is the process of physically damaging the media so that it is not usable as media, and so that no known method can retrieve data from it.

3.2.2. Only approved equipment and overwriting software that is compatible with the specific hardware for overwriting shall be used to clear media that have contained classified information. Use of such software shall be coordinated in advance with the DAA. The success of the overwrite procedure shall be verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) shall remain at the previous level of classification and remain in a secure, controlled environment.

3.2.3. Overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with *declassification*. Declassification is the separate administrative process resulting in a determination that given media no longer requires protection as classified information. Procedures for declassifying media require DAA approval.

a. Overwriting Media: Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing.
    1) Several factors can reduce the effectiveness of overwriting, These include ineffectiveness of the overwrite procedures, equipment failure (e.g., misalignment of read/write heads), and inability to overwrite bad sectors or tracks or information in inter-record gaps.

2) To clear magnetic disks, overwrite all locations three times time with a random character, the second time with a character, and the third time with the complement of that character).

b. Degaussing Media: Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

1) Magnetic media are divided into three types based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. Type I degaussers are used to degauss Type I media (i.e., media whose coercivity is no greater than 350 Oersteds [Oe]). Type IIa degaussers are used to degauss Type Ha media (i.e., media whose coercivity is no greater than 900 Oe). Currently, no degaussers can effectively degauss all Type III media (i.e., media whose coercivity is over 900 Oe). Some degaussers are rated up to 1700 Oe, but their specific approved rating must be determined prior to use. The correct use of degaussing products improves assurance that data is no longer retrievable and that inadvertent disclosure will not occur.

2) Refer to the current issue of NSA's Information Systems Security Products and Services Catalogue (Degausser Products List Section) for the identification of degaussers acceptable for the procedures specified in this manual. The vendor will provide test procedures to verify continued compliance. The ISSM, using these vendor-supplied test procedures, shall ensure testing at least annually of these products to verify that they continue to meet their manufacturers' specifications.

c. Sanitizing Media: Sanitization removes information from media or equipment so that data recovery using any known technique or analysis is prevented. Sanitizing is a two-step process that includes removing data from the media by effectively degaussing the media and removing all sensitivity labels, markings, and activity logs. After magnetic media are properly degaussed in accordance with NSA/CSSM 130-2, and all identifying labels removed, they are considered to be sanitized.

3.2.4. Recycle Media containing classified information.

a. *Reuse of media.* Cleared or sanitized media that has previously contained classified information may be reused at the same classification level (e.g., TS -> TS), or at a higher level (e.g., S -> TS). Sanitized media may be downgraded or declassified with the DAA's and, as applicable, the Data Owner's approval as specified in the SSAA/SSP. Only approved equipment and software shall be used to overwrite and degauss magnetic media containing classified information. Each action or procedure taken to overwrite or degauss such media shall be verified.

b. Sanitizing. Magnetic media containing classified information can be sanitized by use of an approved degaussing procedure. The DAA, with the Data Owner's approval (if applicable), can allow overwriting of some types of classified information as a sanitizing procedure.

c. Overwriting cannot sanitize media that have ever contained Sensitive Compartmented Information, other intelligence information, TOP SECRET SAP information, or Restricted Data; such media shall be degaussed before release.

3.2.4.1. Media that has ever contained COMSEC material cannot be sanitized at all; it shall be destroyed before release in compliance with national and NASA COMSEC destruction procedures.

3.2.5. Optical Disks. Optical disks (including compact disk/read only memory, write once/read many. Digital Versatile Disk, and writeable compact discs) offer no mechanism for sanitization and must be destroyed via incineration or any other NSA-approved method. They should be placed in a CLASSIFIED trash bag labeled "non-soluble" and disposed as CLASSIFIED waste.

3.2.6. Destroying Media. Data storage media will be destroyed in accordance with approved methods.

3.2.7. Malfunctioning Media. Magnetic storage media that malfunctions or contains features that inhibit overwriting or degaussing shall be reported to the ISSO, who will coordinate repair or destruction with the responsible DAA.

3.3 Examination of Hardware and Software.

3.3.1. NSS hardware and software shall be examined when received from the vendor and before being placed into use.

3.3.2. IS Software. Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the NSS. Security-related software shall be tested to verify that the security features function as specified.

3.3.3. IS Hardware. Hardware shall be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the NSS when placed under facility control and cognizance. Subsequent changes and developments that affect security may require additional examination.

3.3.4. Release of Memory Components and Boards: Before the release of any components or boards from an area used to process or store classified information, whether because they are malfunctioning or because they are no longer needed) the requirements of subsections 3.3.4.2 (b) and (c), below, shall be met. This section applies only to components identified by the vendor or other technically-knowledgeable individual as having the capability of retaining user-addressable data and does not apply to other items (e.g., cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this document, a memory component is the Lowest Replaceable Unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

3.3.4.1. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release (see NSA Manual 130-2). Memory components are specifically handled as either volatile or nonvolatile, as described below.

a. *Volatile Memory Components*. Memory components that do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system that do not contain residual data, are considered volatile memory components. Volatile components that have contained classified information may be released only in accordance with procedures developed by the ISSO and stated in the SSAA/SSP. A record shall be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remains in or on the component when power is removed.
b. *Nonvolatile Memory Components*. Components that do retain data when all power sources are discontinued are nonvolatile memory components; these include read-only memory (ROM), programmable ROM (PROM), or erasable PROM (EPROM), and their variants. Those that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components may be released after successful completion of the procedures outlined in NSA/CSSM 130-2. Failure to accomplish these procedures shall require the ISSO to coordinate with the DAA for a determination of releasability.

3.3.4.2. Release of Systems and Components. The ISSO shall develop equipment removal procedures for systems and components that have processed or contained classified or extremely sensitive information; these procedures shall be stated in the SSAA/SSP. When such equipment is no longer needed, it can be released after:

a. Inspection of the system equipment by the ISSO or designee. This review shall assure that all media, including internal disks, have been removed or sanitized.
b. Creation of a record of the equipment release indicating the procedure used for sanitization, and to whom the equipment was released. This record shall be retained for a period prescribed by the DAA.
c. Using procedures specified by the DAA, notification to the DAA of the release of the equipment.

3.4 Identification and Authentication Management

3.4.1. As the complexity of a specific NSS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSAA/SSP.

3.4.2. Unique Identification. Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.

3.4.3. Authentication at Logon. Users shall be required to authenticate their identities at “logon” time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

3.4.4. Applicability of Logon Authentication. In some cases, it may not be necessary to use IS security controls as logon authenticators. In the case of stand alone workstations, or small local area networks, physical security controls and personnel security controls may suffice. For example, if the following conditions are met, it may not be necessary for the IS to have a logon and password:

a. The workstation does not have a permanent (internal) hard drive, and the removable hard drive and other associated storage media are stored in an approved security container when not in use.
b. All of the users with access to the workstation, the security container, and removable media have the required clearance level and need-to-know for all of the data processed on the workstation.
c. The workstation is located within an approved security area, and all uncleared/lower-cleared personnel are escorted within the area.

3.4.5. Access to Authentication Data. Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.

3.4.6. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.

3.4.7. User ID Removal. When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual’s user ID and its authentication shall be disabled or removed from the system.

3.4.8. User ID Revalidation. Active user IDs shall be revalidated at least annually.

3.4.9. Protection of Individual Authenticator. An authenticator that is in the form of knowledge (password) or possession (smart card, keys) shall not be shared with anyone.

3.4.10. Protection of Individual Passwords. When passwords are used as authenticators, the following shall apply:

a. Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.
b. Passwords shall contain a minimum of eight non-blank characters, shall be valid for no longer than three months and changed when compromised.
c. Passwords shall be generated by a method approved by the DAA. Password acceptability shall be based on the method of generation, the length of the password, password structure, and the size of the password space. The password generation method, the

length of the password, and the size of the password space shall be described in an attachment to the SSAA/SSP.

3.4.11. When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

3.4.12. User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., SYSTEM, TEST, and MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO shall also ensure that these passwords are changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

3.5 Maintenance

3.5.1 NSS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

3.5.2. *Cleared Maintenance Personnel*. Maintenance personnel who are cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.

3.5.3. *Uncleared (or Lower-Cleared) Maintenance Personnel.*

3.5.3.1. If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.

3.5.3.2. System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.

3.5.3.3. Prior to maintenance, the NSS shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared, procedures (which are identified in the SSAA/SSP) shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the system.

3.5.3.4. A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED—FOR MAINTENANCE

ONLY" and protected in accordance with procedures established in the SSAA/SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

3.6 Malicious Code

3.6.1. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.

3.7 Marking Hardware, Output, and Media

3.7.1. Markings on hardware, output, and media shall conform to national security policy and NPR 1600.1. If the required marking is impractical or interferes with the operation of the media, the DAA may approve alternate marking procedures.

3.7.2. Hardware Components. All components of an IS, including input/output devices that have the potential for retaining information, which includes terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS. The exception would be when operations security (OPSEC) dictates otherwise, and shall be so stated in the SSAA/SSP. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen. If the DAA requires that labels be color coded to indicate classification level they shall be orange for Top Secret, red for Secret, blue for Confidential, and green for unclassified.

3.7.3. Hard Copy Output and Removable Media. Hard copy output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human-readable, external markings to the accreditation level of the IS unless an appropriate classification review has been conducted or in the case of media, the information has been generated by a tested program verified to produce consistent results and approved by the DAA. Such programs will be tested on a statistical basis to ensure continuing performance.

3.7.4. Unclassified Media. In the DAA-approved areas where classified and unclassified information are processed on co-located IS, unclassified media shall be so marked.

3.8 Personnel Security

3.8.1. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.

3.9 Physical Security

3.9.1. Safeguards shall be established that prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS.

3.9.2. Classified processing shall take place in a DAA-approved area.

3.9.3. Visual Access. NSS devices, that display or output information in human-readable form, shall be positioned to prevent unauthorized individuals from reading the information.

3.9.4. Unescorted Access. All personnel granted unescorted access to the area containing the NSS shall have an appropriate security clearance.

3.10 Protection of Media

3.10.1. Media must be protected to the level of accreditation until an appropriate classification review has been conducted.

3.11 Review of Output and Media

3.11.1. Human-Readable Output Review. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

3.11.2. Media Review**.** Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. DAA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

3.12 Configuration Management

3.12.1. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

3.12.2. Configuration Documentation: Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.

3.12.3. System Connectivity: Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

3.12.4. Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

3.12.5. CM Plan. The facility CM program shall be documented in a CM plan and shall include:

a. Formal change control procedures to ensure the review and approval of security-relevant hardware and software.
b. Procedures for management of all documentation, such as the SSP and security test plans, used to ensure system security.
c. Workable processes to implement, periodically test, and verify the CM plan.
d. A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

CHAPTER 4: NSS REQUIREMENTS PROTECTION MEASURES

4.1 Protection Profiles

4.1.1. Protection profiles required for a particular NSS IS are determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals and need-to-know embodied in the user environment. Provisions for integrity and availability concerns are included in this Chapter to provide guidance when the Government Contracting Activity (GCA) contractually imposes them.

4.2 Level of Concern

4.2.1. The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability.

4.2.2. Information Sensitivity Matrices. The matrices presented in Tables 1, 2, and 3 are designed to assist the DAA, with input from the ISSM in determining the appropriate protection level for confidentiality, and the level of concern for integrity, and availability, if contractually mandated, for a given IS processing a given set of information. The Information Sensitivity Matrices should be used as follows:

a. A determination of high, medium, or basic shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.
b. When multiple applications on a system result in different levels of concern for the categories of confidentiality, integrity and availability the highest level of concern for each category shall be used.

4.2.3. Confidentiality Level of Concern. In considering confidentiality, the principal question is the necessity for supporting the classification levels and the categories of information (e.g., Secret National Security Information) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a Protection Level. The Protection Level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system.

4.2.4. Integrity Level of Concern. In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question.

4.2.5. Availability Level of Concern. In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.

4.3 Protection Level

4.3.1. The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements (tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.

4.3.2. Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.

4.3.3. Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system, i.e. a system high mode.

4.3.4. Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system, i.e. compartmented mode.

4.4 Protection Profile Components

4.4.1. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Chapter 6. Tables 5, 6, and 7 present the requirements detailed in Chapter 6. To use these tables, find the column representing the protection level for confidentiality, or, if contractually mandated, find the column representing the level of concern for integrity or availability.

4.4.2. *Confidentiality Components*: Confidentiality components describe the confidentiality protection requirements that must be implemented in an IS using the profile. The confidentiality protection requirements are graded according to the confidentiality protection levels.

4.4.3. *Integrity Components*: Integrity components, if applicable, describe the integrity protection requirements that must be implemented in an IS using the profile. The integrity protection requirements are graded according to the integrity level of concern.

4.4.4. *Availability Components*: Availability components, if applicable, describe the availability protection requirements that must be implemented in an IS using the profile. The availability protection requirements are graded according to the availability level of concern.

Table 1. Information Sensitivity Matrix for Confidentiality.

Level of Concern	Qualifiers
High	TOP SECRET and SECRET Restricted Data (SIGMAs 1,2,14,15)
Medium	SECRET SECRET Restricted Data
Basic	CONFIDENTIAL

Table 2. Information Sensitivity Matrix for Integrity.

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Basic	Reasonable degree of accuracy required for mission accomplishment.

Table 3. Information Sensitivity Matrix for Availability.

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Basic	Information must be available with flexible tolerance for delay.

NOTE: In this context, “High - no tolerance for delay” means no delay; “Medium - minimum tolerance for delay” means a delay of seconds to hours; and “Basic - flexible tolerance for delay” means a delay of days to weeks. Integrity and availability shall only apply when they have a direct impact on protection measures for confidentiality, i.e., integrity of the password file, integrity of audit logs or when contractually imposed.

Table 4. Protection Level Table for Confidentiality.

Level of Concern	Lowest Clearance	Formal Access Approval	Need-To-Know	Protection Level
High, Medium, or Basic	At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	3
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

Table 5. Protection Profile Table for Confidentiality.

	Confidentiality Protection Level		
Requirements	P L 1	PL 2	PL 3
Audit Capability	Audit 1	Audit 2	Audit 3 Audit 4
Data Transmission	Trans 1	Trans 1	Trans 1
Access Controls	Access 1	Access 2	Access 3
Identification & Authentication	I&A 1	I&A 2,3,4	I&A2,4,5
Resource Control		ResrcCtrl 1	ResrcCtrl 1
Session Controls	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation	Doc 1	Doc 1	Doc 1
Separation of Functions			Separation
System Recovery	SR 1	SR 1	SR 1
System Assurance	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing	Test 1	Test 2	Test 3

Table 6. Protection Profile Table for Integrity.

	Integrity Level of Concern		
Requirements	Basic	Medium	High
Audit Capability	Audit 1	Audit 2	Audit 3
Backup and Restoration of Data	Backup 1	Backup 2	Backup 3
Changes to Data		Integrity 1	Integrity 2
System Assurance		SysAssur 1	SysAssur 2
Security Testing	Test 1	Test 2	Test 3

Table 7. Protection Profile Table for Availability.

	Availability Level of Concern		
Requirements	Basic	Medium	High
Alternate Power Source		Power 1	Power 2
Backup and Restoration of Data	Backup 1	Backup 2	Backup 3

CHAPTER 5: SPECIAL CATEGORIES

5.1 General

5.1.1. Several categories of systems can be adequately secured without implementation of all the technical features specified in this NPR. These systems are not “exceptions” or “special cases” but applying the technical security requirements to these systems will result in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these “special” systems (such as guards or pure servers; and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

5.2 Single-user, Stand-alone Systems

5.2.1. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The DAA can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the DAA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as described below.

5.3 Periods Processing

5.3.1. Periods processing is a method of sequential operation of an IS that provides the capability to process information at various levels of sensitivity at distinctly different times.

5.3.2. Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).

5.3.3. Sanitization After Use. If an IS is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSAA/SSP shall specify the sanitization procedures to be employed by each user before and after each use of the system.

5.3.4. Sanitization Between Periods. The IS shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have an access authorization or need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the

SSAA/SSP. Such procedures could include, among others, sanitizing non-volatile storage, exchanging disks, and powering down the IS and its peripherals.

5.3.5. Media For Each Period. An IS employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

5.3.6. Audit. If there are multiple users of the system and the system is not capable of automated logging, the DAA shall consider requiring manual logging, or upgrading the system to allow automated logging.

5.4 Pure Servers

5.4.1. Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the following characteristics:

a. No user code is present on the system.
b. Only system administrators and maintainers can access the system.
c. The system provides non-interactive services to clients (e.g., packet routing or messaging services).
d. The hardware and/or application providing network services otherwise meet the security requirements of the network.
e. The risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low.
f. The risk of attack against the SSS using physical access to the system itself is sufficiently low.

5.4.2. The platform (i.e., hardware and operating system) on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard or server functional capabilities in a severely constrained way). The guard application or server application itself will have to provide the more stringent technical protections appropriate for the system’s protection level and operational environment. Assurances appropriate to the levels of concern for the system shall be implemented.

5.4.3. Systems that have general users or execute general user code are not “pure servers” within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.

5.4.4. The term “pure server” is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this section and, if such a system meets the specifications in a, above, the system’s technical requirements could be categorized by this section.

5.4.5. The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements) which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines, which shall be documented in the SSAA/SSP.

5.5 Tactical, Embedded, Data-Acquisition, and Special Purpose Systems

5.5.1. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called “embedded” systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first and most importantly, there are no general users on the system; and, second, there is no user code running on the system. If the DAA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The DAA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system’s protection level.

5.6 Systems with Group Authenticators

5.6.1. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group authenticators. In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in SSAA/SSP. Group authenticators may not be shared with anyone outside of the group and shall be kept to an absolute minimum.

5.7 Co-Location of SAP and Unclassified IS

5.7.1. DAA approval is necessary to co-locate classified and unclassified IS’s in a Special Access Program Facility (SAPF). The following conditions shall be adhered to:

a. An IS approved for processing unclassified information must be clearly marked as such when located within a SAPF.
b. An IS approved for processing unclassified information must be physically separated from any classified IS.
c. An IS approved for processing unclassified information must not be connected to any classified IS without the written approval by the NASA HQ PAA.
d. Users must be provided with co-location process and procedures as part of their required

security and awareness training.

e. The ISSO must document in the SSAA/SSP the procedures and technical safeguards to ensure the protection of classified information.

f. All unmarked media must be treated as classified at the highest level processed by the facility until reviewed and verified.

5.7.2. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting DAA and part of the SSAA/SSP.

CHAPTER 6: PROTECTION REQUIREMENTS

6.1 Introduction

6.1.1. This section describes the implementation requirements for different protection measures.

6.2 Alternate Power Source (Power)

6.2.1. An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

6.2.2. Power 1 Requirements. Procedures for the graceful shutdown of the system shall ensure no loss of data. The decision not to use an alternate source of power, such as an un-interruptible power supply (UPS) for the system, shall be documented.

6.2.3. Power 2 Requirements. Instead of Power 1, procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

6.3 Audit Capability

6.3.1. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

6.3.1.1. *Audit 1 Requirements*

a. Automated Audit Trail Creation: The system shall automatically create and maintain an audit trail or log (On a PL-1 system only: In the event that the Operating System cannot provide an automated audit capability, an alternative method of accountability for user activities on the system shall be developed and documented.) Audit records shall be created to record the following:
    1) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.
    2) Successful and unsuccessful logons and logoffs.
    3) Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.
    4) Changes in user authenticators.
    5) The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.
    6) Denial of access resulting from an excessive number of unsuccessful logon attempts.

b. Audit Trail Protection: The contents of audit trails shall be protected against unauthorized access, modification, or deletion.
c. Audit Trail Analysis: Audit analysis and reporting shall be scheduled, and performed. Security relevant events shall be documented and reported. The frequency of the review shall be at least weekly and shall be documented in the SSAA/SSP.
d. Audit Record Retention: Audit records shall be retained for at least one review cycle or as required by the DAA.

6.3.1.2. *Audit 2 Requirements*. In addition to Audit 1:

a. Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual): Periodic testing by the ISSO or ISSM of the security posture of the IS.

6.3.1.3. *Audit 3 Requirements*. In addition to Audit 2:

a. Automated Audit Analysis: Audit analysis and reporting using automated tools shall be scheduled and performed.

6.3.1.4. *Audit 4 Requirements*. In addition to Audit 3:

a. An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions.

6.4 Backup and Restoration of Data (Backup)

6.4.1. The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

6.4.1.1. *Backup 1 Requirements*.

a. Backup Procedures: Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, shall be documented.
b. Backup Frequency: The frequency of backups shall be defined by the ISSM and documented in the backup procedures.

6.4.1.2. *Backup 2 Requirements*. In addition to Backup 1:

a. Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or off facility, so as to reduce the possibility that a common occurrence could eliminate the on-facility backup data and the off-facility backup data.
b. Verification of Backup Procedures. Backup procedures shall be periodically verified.

6.4.1.3. *Backup 3 Requirements*. In addition to Backup 2:

a. Information Restoration Testing: Incremental and complete restoration of information from backup media shall be tested on an annual basis and documented in the SSAA/SSP.

6.5 Changes to Data (Integrity)

6.5.1. The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

6.5.1.1. *Integrity 1 Requirements*.

a. Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes.

6.5.1.2. *Integrity 2 Requirements*. In addition to Integrity 1:

a. Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data and IS software changes and the off-line verification of all changes at all times.

6.6 Data Transmission (Trans)

6.6.1. Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

6.6.1.1. *Trans 1 Requirements*.

a. Protections. One or more of the following protections shall be used.
b. Information distributed only within an area approved for open storage of the information.
c. National Security Agency (NSA)-approved encryption mechanisms appropriate for the encryption of classified information.
d. Protected Distribution System.

6.7 Access Controls (Access)

6.7.1. The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

6.7.1.1. *Access 1 Requirements*.

a. Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

6.7.1.2. *Access 2 Requirements*. In addition to Access 1:

a. Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

6.7.1.3. *Access 3 Requirements*. In addition to Access 2:

a. Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.
b. Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

6.8 Identification and Authentication (I&A)

6.8.1.1. *I&A 1 Requirements*

a. Procedures that include provisions for uniquely identifying and authenticating the users.
b. Procedures can be external to the IS (e.g., procedural or physical controls) or internal to the IS (i.e., technical). Electronic means shall be employed where technically feasible.

6.8.1.2. *I&A 2 Requirements*. In addition to I&A 1:

a. An I&A management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified in the SSP:
    1) Initial authenticator content and administrative procedures for initial authenticator distribution.
    2) Individual and Group Authenticators. Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator.
    3) Length, composition and generation of authenticators.
    4) Change processes (periodic and in case of compromise.
    5) Aging of static authenticators (i.e., not one-time passwords or biometric patterns).
    6) History of authenticator changes, with assurance of non-replication of individual authenticators.
    7) Protection of authenticators.

6.8.1.3. *I&A 3 Requirements*. In addition to I&A 2:

a. Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

6.8.1.4. *I&A 4 Requirements*. In those instances where the means of authentication is user-specified passwords, the ISSM may employ (with the approval of the DAA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

6.8.1.5. *I&A 5 Requirements*. In those instances where the users are remotely accessing the IS, the users shall employ a strong authentication mechanism.

6.9 Resource Control (ResrcCtrl)

6.9.1. The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

6.10 Session Controls (SessCtrl)

6.10.1. Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user's session.

6.10.1.1. *SessCtrl 1 Requirements*.

a. User Notification. All users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits each initial screen (displayed before user logon), it shall contain a warning text to the user and the user shall be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection and analysis of audit trail information, shall be performed). The DAA will provide an approved banner. If it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the DAA.
b. Successive Logon Attempts. If the operating system provides the capability, successive logon attempts shall be controlled as follows:
   1) By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID.
   2) By limiting the number of access attempts in a specified time period.
   3) By the use of a time delay control system.
   4) By other such methods, subject to approval by the DAA.
c. System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions

are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

6.10.1.2. *SessCtrl 2 Requirements*. In addition to SessCtrl 1:

a. Multiple Logon Control. If the IS supports multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall be a single logon session.
b. User Inactivity. The IS shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSAA/SSP.
c. Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user’s last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID, since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

6.11 Security Documentation (Doc)

6.11.1. Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSAA/SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSAA/SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSAA/SSP.

6.11.1.1. *Doc 1 Requirements*.

a. SSAA/SSP. The SSAA/SSP shall contain the following:
   1) System Identification.
   2) Security Personnel. The name, location, and phone number of the responsible system owner, DAA, ISSM, and ISSO.
   3) Description. A brief narrative description of the system or network mission or purpose and architecture, including sub networks, communications devices, and protocols.
b. System Requirements Specification.
   1) Sensitivity and Classification Levels. The sensitivity or classification levels, and categories of all information on the system and clearance, formal access approval and need-to-know of IS users.

2) Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.
3) Protection Measures. Identify protection measures and how they are being met.
4) Variances from Protection Measure Requirements. A description of any approved variances from protection measures. A copy of the approval documentation shall be attached to the SSP.

c. System-Specific Risks and Vulnerabilities: A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the facility or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.

d. System Configuration: A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems, and an information flow diagram.

e. Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary when a person other than the DAA responsible for this system approves systems. A copy of any memoranda of understanding with other agencies shall be attached to the SSAA/SSP.

f. Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

g. Certification and Accreditation Documentation.
1) Security Testing. Test plans, procedures, and test reports including risk assessment.
2) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.
3) Certification. A certification statement stating that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the ISSM.
4) Accreditation. Documentation for accreditation includes the certification package. The DAA approves the package and provides accreditation documentation.

6.12 Separation of Function Requirements (Separation)

6.12.1. At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by the same person.

6.13 System Recovery (SR)

6.13.1. System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

6.13.1.1. *SR 1 Requirements.*

a. Procedures and IS features shall be implemented to ensure that IS recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the IS shall be accessible only via terminals monitored by the ISSO or his /her designee, or via the IS console.

6.14 System Assurance (SysAssur)

6.14.1. System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy (or policies) of the system, (e.g. Security Support Structure (SSS)).

6.14.1.1. *SysAssur 1 Requirements.*

a. Access to Protection Functions. Access to hardware/software/firmware that performs systems or security functions shall be limited to authorized personnel.

6.14.1.2. *SysAssur 2 Requirements.* In addition to SysAssur1:

a. Protection Documentation. The protections and provisions of the SysAssur shall be documented.
b. Periodic Validation of SysAssur. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS and shall be documented in the SSAA/SSP.

6.14.1.3. *SysAssur 3 Requirements*. In addition to SysAssur2:

a. SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures).

6.15 Security Testing (Test)

6.15.1. Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM is responsible for the required test being performed and documented.

6.15.1.1. *Test 1 Requirements*.

a. Assurance shall be provided to the DAA that the system operates in accordance with the approved SSAA/SSP and that the security features, including access controls and configuration management, are implemented and operational.

6.15.1.2. *Test 2 Requirements.* In addition to Test1:

a. Written assurance shall be provided to the DAA that the IS operates in accordance with the approved SSAA/SSP, and that the security features, including access controls, configuration management and discretionary access controls, are implemented and operational.

6.15.1.3. *Test 3 Requirements.* In addition to Test2:

a. Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.
b. A test plan and procedures shall be developed and shall include:
    1) A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.
    2) A detailed description of the assurances that have been implemented, and how this implementation will be verified.
    3) An outline of the inspection and test procedures used to verify this compliance.

6.16 Disaster Recovery Planning

6.16.1. The ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures, which shall be annotated in the SSAA/SSP.

CHAPTER 7: INTERCONNECTED SYSTEMS

7.1 Interconnected Systems Management

7.1.1. The characteristics and capabilities of an IS implemented as networks require special security considerations. This chapter states additional requirements on a network or expands on the security requirements stated in Chapter 6 as they apply to a network.

7.1.2. When connecting two or more networks, the DAA shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

7.1.3. A unified network is a connected collection of systems or networks that are accredited (1) under a single SSAA/SSP, (2) as a single entity, and (3) by a single DAA. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single DAA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

7.1.4. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

7.1.5. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:

a. They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or
b. Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or
c. Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

7.1.6. Any IS connected to another system that does not meet either d (2) or d (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:

a. A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.
b. A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.
c. Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the CI shall notify the user of the communication and forward the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

7.2 Controlled Interface (CI) Functions

7.2.1. The functions of the CI include:

a. Providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts.
b. Providing a reliable exchange of security-related information.
c. Filtering information in a data stream based on associated security labels for data content.

7.2.2. CI’s have several characteristics including the following:

a. There are no general users on the CI.
b. There is no user code running on the CI.
c. The CI provides a protected conduit for the transfer of user data.
d. Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

7.3 Controlled Interface Requirements

7.3.1. The CI shall have the following properties:

a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.
b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.
c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or IS.
d. User Code. The CI shall not run any user code.
e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.

7.3.2. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

7.4 Assurances for CI's

7.4.1. Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation alone.

CHAPTER 8: Communications Security (COMSEC)

8.1 General

8.1.1. The National Security Agency (NSA)/Central Security Service is America's cryptology organization. It coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. NSA employs the country's premier cryptologists. It is said to be the largest employer of mathematicians in the United States and perhaps the world. Its mathematicians contribute directly to the two missions of the Agency: designing cipher systems that will protect the integrity of U.S. information systems and searching for weaknesses in adversaries' systems and codes.

8.1.2. NSA is the executive agent for developing and implementing national level policy affecting the control of COMSEC material to protect classified information. NSA is also responsible for the production and distribution of most COMSEC material used to secure communications as well as the development and production of cryptographic equipment.

8.2 COMSEC Material Control System (CMCS)

8.2.1. The protection of vital and sensitive information moving over government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of operations. To this end, a system has been established to distribute, control, and safeguard COMSEC material. This national system managed by NSA consists of production facilities, COMSEC Central Offices of Records (COR's), distribution facilities (i.e., depots), and COMSEC accounts, is known collectively as the Consolidated Material Control System (CMCS).

8.2.2. NASA administers its own CMCS under the auspices of the NSA, which includes government and contractor based CMCS Accounts, within its area of responsibility. The NASA system implements national policy, publishes procedures, establishes its own COMSEC accounts, and provides a COR to account for COMSEC material.

8.2.3. Because COMSEC materials and equipment (e.g., secure telephones) protect our nation's most sensitive national security interests, they require special processes, special clearances and access. Only individuals with a special need-to-know shall have access to COMSEC materials and equipment. Therefore, NASA COMSEC materials and equipment shall participate in the national CMCS process for accountability and shall not be introduced into the NASA Equipment Management System (NEMS).

8.3 Central Office of Record (COR)

8.3.1. The COMSEC COR is the office of a federal department or agency that keeps records of "accountable" Communications Security (COMSEC) material held by elements subject to its oversight. The NASA COR is located at Kennedy Space Center (KSC) and is directly responsible to the Director, Security Management Division or his/her designated representative, NASA HQ Office of Security and Program Protection. It administers the NASA COMSEC program and acts as the COR for all NASA COMSEC. The NASA COR has overall COMSEC control and authority to carry out and meet national security policy and procedures. The COR is responsible for all COMSEC material, training and operating procedures as outlined in this chapter.

8.3.2. As a minimum, the NASA COR shall:

a. Administer the NASA COMSEC program and acts as the COR for all NASA accounts.
b. Operate and maintain the NASA COR, which exercises daily administrative, operational, and technical control over NASA COMSEC Accounts.
c. Draft and publish policy directives, standards, bulletins, and procedures pertaining to COMSEC material security, distribution, training, handling, destruction and accounting within NASA.
d. Be responsible for the establishment and publication of COMSEC Standard Operating Procedures (CSOP's) that detail how the COMSEC program within NASA is executed. CSOP's shall be signed by NASA Headquarters, OSSP, numbered, and are authoritative in nature. They shall prescribe the minimum policies and procedures for issuing, accounting, handling, safeguarding, and disposing of COMSEC material. The COR shall monitor compliance with National Standards for the application of cryptographic and physical security measures to properly protect COMSEC materials and facilities.
e. Develop procedures for and monitor compliance with proper physical storage and account management of COMSEC material.
f. Monitor compliance with national standards of the Protective Packaging Program for cryptographic keying material.
g. Conduct inspection on each account to ensure national and local policy compliance.
h. Establish and disestablish NASA COMSEC accounts.
i. Provide status of NASA COMSEC materials to NASA HQ Office of Security and Program Protection (OSPP).
j. Provide disposition instructions for NASA COMSEC material.
k. Evaluate instances of loss, compromise, and procedural violations of COMSEC procedures to determine the adequacy of existing procedures as well as overall compliance with existing policy.
l. Receive, verify, store, and ship COMSEC material in support of NASA requirements.
m. Manage the NASA COMSEC Training Program.

8.4 COMSEC Account Manager (CAM)/Alternate CAM

8.4.1. There shall be a COMSEC Account Manager (CAM) and Alternate CAM (ACAM) for each NASA COMSEC account, one of which shall be a government civil service employee. The NASA CAM is the individual primarily responsible for all “accountable” COMSEC material issued to an account. That individual is the COMSEC Custodian, or, within NASA, the COMSEC Account Manager. The CAM must personally sign for receipt and custody of each “accountable” COMSEC item issued to the account. The CAM shall report all activities to the NASA COR to include incidents involving COMSEC material. Individuals appointed as a CAM shall not have other duties assigned that would interfere with the strict responsibilities required of the CAM position. If the CAM duties are assigned to an individual as an additional duty to their normal position, their supervisor and management must be made aware of the strict nature of COMSEC accountability and support to National Security.

8.4.2. COMSEC Account Managers (CAM’s) are responsible for the proper management and security of all COMSEC material held at the location. For all COMSEC activities, the CAM is directly responsible to the chief of security at each NASA Center and location.

8.4.3. Specific guidance is located in the CSOP’s provided by the NASA COR, These CSOP’s are the governing authority for all functions for the CAM and the proper operation of their accounts. All NASA CAM’s/ACAM’s shall be trained to meet the requirements of established by national policies, NASA guidance, and COR Standard Operating Procedures (CSOP) and bulletins.

8.4.4. CAM’s shall work directly with the NASA COR for assistance and guidance with the operation of their accounts.

8.4.5. As a minimum, the CAM shall:

a. Provide the local users and/or other interested personnel (with appropriate clearances and need-to-know) with information about new or revised COMSEC policies and procedures and their impact.
b. Acquire, monitor, and maintain the account COMSEC material allowance. This includes a semi-annual review of all COMSEC material holdings to ensure that there is a continuing need for the quantity and types of all COMSEC material held.
c. Maintain proper storage and adequate physical security for the COMSEC material held by the account.
d. Keep Alternate COMSEC Account Manager (ACAM) informed of the status of the account so that the Alternate is, at all times, fully capable of assuming the duties of the CAM.
e. Provide users / local elements written guidance or appropriate extracts from this publication concerning and / or CSOP information on the handling, accountability, and the disposition of COMSEC material. Emphasis must be placed on material accountability, Two-Person-Integrity (TPI) requirements, security, and the identification of improper practices.

e. Conduct training to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures.
f. Maintain records and files as required and outlined in the CSOP's.
g. Ensure prompt and accurate preparation, signature, and submission of account correspondence, message, and accounting reports.
h. Issue COMSEC material on local custody form(s)/hand receipts after the CAM verifies that the recipient is authorized to hold COMSEC material and has executed a COMSEC Responsibility Acknowledgment Form.
i. Oversee the implementation of and compliance with Over-The-Air-Rekey / Over-The-Air-Transfer (OTAR/OTAT) procedures (e.g., periodic review of local logs, adherence to TPI requirements).
j. Ensure that users / local elements properly inventory and destroy COMSEC material issued to them through periodic documented spot checks.
k. Maintain the account's portion of the Emergency Action Plan (EAP).
l. Conduct required inventories and destruction of COMSEC material.
m. Ensure that proper physical security measures are maintained when COMSEC material is transported.
n. Ensure that COMSEC material shipped outside of the center is properly packaged and shipped via an authorized method.
o. Ensure that TPI requirements are maintained in accordance with this manual.
p. Report immediately any incidents to: as described in section 8.5.

8.4.6. Specific CAM/ACAM duties and responsibilities are spelled out by NASA CSOP to include the nomination and appointment process to and by the NASA COR.

8.5 COMSEC Incidents Reporting and Handling

8.5.1. COMSEC Incidents must be reported in accordance with NSTISSI 4003, Reporting and Evaluating COMSEC Incidents. The NASA COR also serves as the COMSEC Monitoring Activity for NASA related COMSEC incidents and the applicable NASA CSOP provides more specific details on reporting and handling of COMSEC incidents within NASA. Existence of the NASA CSOP for COMSEC Incident Reporting and Handling does not relieve personnel with COMSEC responsibilities from being thoroughly familiar with the requirements of NSTISSI 4003. CSOP's supplement the requirements of NSTISSI 4003 and provides additional guidance, as required. Any conflict between the governing CSOP and NSTISSI 4003 will be resolved in favor of NSTISSI 4003. The reporting requirements of NSTISSI 4003 and the governing CSOP cover all COMSEC material, regardless of form or generation process.

8.6 Electronic Key Management System (EKMS)

8.6.1. The Electronic Key Management System (EKMS) System is a NSA led program comprised of multiple tiers responsible for electronic Communications Security (COMSEC) key management, accounting and distribution. Specifically, EKMS generates and distributes electronic key materiel for NSA encryption devices, whose keys are loaded using standard fill devices, and directs the distribution of NSA produced Key materiel. Additionally, EKMS performs account registration, privilege management, ordering, distribution and accounting to direct the management and distribution of physical COMSEC materiel.

8.6.2. EKMS Tier 2. The NASA COR, under the auspice of the OSPP, shall serve as the central point of management and operations for implementation of EKMS within NASA. As a minimum, the COR shall perform the following:

c. Operate and maintain in compliance with NSA policies and doctrine the NASA EKMS Tier 2 platform composed of a commercial off-the-shelf (COTS) personal computer (PC) running the Santa Cruz Operation's SCO UNIX operating system called a Local Management Device (LMD), a NSA KOK-22A Key Processor (KP), NSA-supplied Local COMSEC Management Software (LCMS), and approved connecting cables and fill devices (e.g., Data-Transfer-Device).
d. Ensure that LMD/KP's with LCMS are certified and accredited prior to their operation by an appropriate NASA Designated Approving Authority (DAA) in compliance with NASA and national security policy directives and requirements.
e. Establish and maintain a CSOP(s) for NASA EKMS operations and utilization.
f. Ensure that users of NASA LMD/KP systems and EKMS fill devices are only operated by authorized and trained individuals, who have been assigned key management responsibilities (e.g., assigned to the COMSEC account). These individuals must have a minimum of a SECRET clearance and be Cryptographic Access Briefed. Final TOP SECRET clearances are necessary to output unencrypted TOP SECRET key as well as to input or output encrypted key at a TOP SECRET account. Person's assigned primary responsibility for the key processed by the LMD/KP must be trained in an authorized EKMS training course and in proper security procedures.
g. Ensure all categories of keys (e.g., externally required, internal, generated, and filled) handled by the KP are properly protected throughout their entire life-cycle.
h. Ensure there is an established and properly functioning "Site Reinitialization" process, which enables the archiving and recovery of all protected data, stored on the LMD and is used when a KP must be replaced with a new KP due to failure or recertification.
i. Ensure there is a functional EKMS "Changeover" process used to re-encrypt the LMD database when the "cryptoperiod" of the Key Encryption Key Local (KEKL) expires.
j. Perform and manage annual electronic rekey of the KP FIREFLY Vector set, or whenever directed by a competent authority (e.g., NSA).
k. Post and manage credentials with the NSA Central Facility or other EKMS elements, depending on user key requirements.
l. Use NSA-approved Type-1 encryption devices or protected distribution systems to provide security for all LMD transmissions over a communications circuit. Such Type-1 encryption devices shall be compatible with the LMD, as well as keyed and NSA endorsed to secure in accordance with the applicable system high classification level.
m. Periodically review LCMS audit records for anomalies. These anomalies shall include instances of multiple invalid logon attempts, invalid file access attempts,

operators logging on at unusual times, excessive transfer of keys to DTD's or other fill devices, etc. When it becomes available, the use of NSA's Audit Reduction Analyzer tool is mandatory. Review LCMS audit data at least monthly, and as part of the change of COMSEC manager process.

n. Ensure that Individuals who analyze LCMS audit data are knowledgeable in LMD/KP operations and trained to detect and respond to anomalous events. Restrict access to audit data to OSPP personnel or designated representatives, Information Systems Security Officer (ISSO), System Administrators (SA), and NSA authorized individuals.

o. Ensures the SA implements approved antivirus tools and software, per guidance of NSA, on the LMD/KP. The COR shall also ensure that the SA receives current signature files from an approved source that are maintained on the system and users are knowledgeable of and use the antivirus process.

p. Provide guidance for the classification, marking, handling, and accountability of EKMS components and key to include the KP, LMD, LCMS, magnetic media, peripheral equipment, and generated key.

q. Ensure that all EKMS key production equipment including KP's is properly packaged and transported by Defense Courier Service (DCS) or cleared courier.

r. Provide guidance and ensure that only the Air Force Cryptologic Support Group (CPSG) performs maintenance on the KP and maintainers of the LMD computer software and storage media have at least a SECRET clearance.

s. Ensure that EKMS Emergency Destruction plans provide for the KP to be zeroized before attempting to destroy the LMD because the KP is more critical to EKMS security. The plans shall also stipulate that unencrypted key be destroyed before encrypted key.

8.6.3. For more information about NASA's implementation of the NSA EKMS Program and electronic key fill devices, contact the NASA COR and obtain the most current copy of the applicable NASA CSOP.

CHAPTER 9: Orbital and Sub-Orbital Space Systems and Platforms

9.1 General

9.1.1. Presidential Decision Directive (PDD) No. 49, Subject: National Space Policy, dated 19 September 1996, has established that U.S. space activities are critical to the national security of the United States. Civil and commercial space activities are also closely linked to the operation of the U.S. Government's critical infrastructures as identified in Presidential Decision Directive (PDD) No. 63, Subject: Critical Infrastructure Protection, dated 22 May 1998, and may, on occasion, be leveraged to satisfy national security requirements. Based on the importance of these activities, it is imperative that a comprehensive, national-level information assurance (IA) space policy be developed, promulgated, and adopted that will ensure the confidentiality, authenticity, integrity, availability, and survivability of associated communications and communications networks under a wide range of peace or war time cyber threat scenarios.

9.1.2. The NASA HQS OSPP has the ultimate authority and oversight regarding the protective measures involving classified national security information (CNSI), regardless of form, to include NASA owned and managed orbital and sub-orbital space systems and platforms within the scope of this NPR. The scope of this chapter of the NPR applies to all NASA orbital and sub-orbital space systems and platforms to include unmanned aerial vehicles (UAV's) and balloons, components or services used by NASA to collect, generate process, store, and display, transmit, or receive national security or sensitive information. It includes launch vehicles, satellites, payloads, launch and test ranges, satellite and network operation centers, and user equipment involving national security related activities.

9.1.3. This policy applies to the planning, budgeting, requirements generation, research, development, testing, evaluation, production, acquisition, deployment, maintenance, life cycle support, education, training, exercises, operations, employment, and oversight of IA activities that are integral to the orbital and sub-orbital space systems and platforms used by NASA. Information and data that transit these systems and platforms shall be protected (e.g., encryption for confidentiality) based upon risk, threat, and vulnerability assessments. This NPR also applies to *Interfaces* between these systems covered by this NPR and external systems when it is determined that the architecture of the system does not provide for adequate protection against potential threats, risks, and vulnerabilities from interconnected, external systems. All NASA-owned or controlled orbital and sub-orbital space systems and platforms within the scope of this NPR shall meet the IA requirements contained herein for compliance with PDD 49, as amended or revised, and NSTISSP No. 12.

9.1.4. Nothing in this NPR shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations.

9.1.5. This policy also serves to remind users of orbital and sub-orbital space systems and platforms outside the national security community that they may also wish to factor IA into those space activities associated with the operation and/or maintenance of critical NASA missions.

9.2 Definitions

9.2.1. Terms used in this chapter of the NPR are defined in Committee on National Security Systems Instruction No. 4009

9.3 Certification and Accreditation

9.3.1. NASA owned and managed orbital and sub-orbital space systems and platforms, supporting CNSI, shall be certified and accredited in compliance with other applicable chapters of this NPR and shall have a duly appointed DAA, CA, an other C&A personnel, as deemed necessary. IA shall be defined and updated throughout their system life cycle in the applicable SSAA/SSP. The status of the IA C&A package and IA-related deliverables shall be a required review item for all major acquisition milestone reviews beginning with the key decision point associated with approval to enter into risk reduction and design development activities. IA shall be a visible element of all orbital and sub-orbital space systems and platforms investment portfolios. Data shall be collected to support reporting and IA management activities across the investment life cycle.

9.3.2. Legacy systems and platforms shall have a DAA assigned to adjudicate any significant IA issues that may arise. Interconnections of Intelligence Community (IC) systems with NASA owned and managed orbital and sub-orbital space systems and platforms shall be certified and accredited in accordance with a process jointly developed by the applicable IC Chief Information Officer (CIO) and the NASA HQS OSPP. For those space systems that transmit, store, or process SCI or other intelligence information under the purview of the DCI, the C&A requirements of DCI Directive 6/3 shall apply.

9.4 Threat, Risk and Vulnerability Assessments

9.4.1. NASA Program/Project Managers shall conduct and coordinate all threat, risk, and vulnerability assessments with the NASA HQS OSPP to determine the current and projected full-range of threats related to these assets. NASA HQS OSPP shall oversee and manage all threat activities associated or related to the Intelligence Community (e.g., CIA, DIA, NRO, and NSA).

9.4.2. Program/Project Managers and key decision makers shall possess appropriate personnel security clearances in order to collaborate and obtain threat data from Office of Security and Program Protection, receive and provide security briefings, and make fully informed risk management decisions based on current threat data to mitigate and accept space system vulnerabilities.

9.5 Information System Security Engineering (ISSE)

9.5.1. IA shall be applied in a balanced manner by performing Information System Security Engineering (ISSE) as an integral part of the system or platform architecture and system engineering process to address all IA requirements in the intended operational environment. Defense-in-depth measures shall be designed into all NASA owned and managed orbital and sub-orbital space systems and platforms, which shall include deterrence, detection, recovery, and reporting capabilities to: counter attacks or security lapses; detect, characterize, and locate the source of an attack; recover from any damage sustained; and quickly alert command authorities via secure communications of any security lapses or attacks. These IA measures help ensure mission success and contribute to satisfying the protection of CNSI.

9.6 Command Links

9.6.1. The command links to NASA-owned or managed orbital and sub-orbital space systems and platforms, supporting CNSI, shall be encrypted and authenticated on an end-to-end basis using National Security Agency (NSA)-approved or NSA-recommended cryptography.

9.6.2. Data generated onboard orbital and sub-orbital space systems and platforms (e.g., telemetry and mission data), which is CNSI, shall be end-to-end encrypted using NSA-approved or NSA-recommended cryptography.

9.6.3. All links (e.g., command uplinks, downlinks, and cross-links) on NASA-owned or controlled orbital and sub-orbital space systems and platforms, which contains CNSI, regardless of transmission media (radio frequency, optical, etc.), shall have transmission security (TRANSEC) protection appropriate for the mission and the projected threat environment over the life of the system. The TRANSEC protection measures used shall be reviewed and approved by the NASA HQS OSPP for the intended application.

9.6.4. Booster telemetry links shall not be encrypted. Emergency, backup links that are automatically invoked to rectify lost communications with malfunctioning satellites need not be encrypted.

9.6.5. A Flight Termination System that uses a Secure Command Destruct System employing NSA-approved cryptography shall be required for all launch vehicles used to deploy NASA-owned or controlled space platforms, which involve CNSI.

9.6.6. Any capability designed into NASA-owned or controlled orbital and sub-orbital space systems and platforms to bypass, for any reason, link protection measures required by this policy during system operation shall minimize the probability of bypass activation due to either malicious acts or random failures. The bypass design shall be submitted to the NASA HQS OSPP for review and comments early in the preliminary design phase, which will coordinate with the Director of National Security Agency (DIRNSA). The bypass design shall be submitted to NASA HQS OSPP to coordinate with DIRNSA for final approval well in advance of the system critical design review to allow the DIRNSA to respond with comments or approval prior to the system critical design review date. Provisions shall also be made for the DIRNSA to review how the bypass was actually implemented in the operational system to ensure that no inadvertent flaws were introduced.

9.7 Commercial-off-the-shelf (COTS)

9.7.1. Commercial-off-the-shelf (COTS) IA or IA-enabled information technology (IT) products (i.e., hardware, software, and firmware) being considered for use on NASA-owned or controlled orbital and sub-orbital space systems and platforms within the scope of this NPR shall be limited to products that have been evaluated and validated in accordance with the requirements of National Security Telecommunications and Information System Security Policy No.11, or for which waivers have been obtained and approved by the NASA HQS OSPP.

9.8 Continuity of Operations Plan

9.8.1. Every NASA-owned or controlled orbital and sub-orbital space systems and platforms within the scope of this NPR relating to critical national security infrastructure shall have a continuity of operations plan and procedures that account for the availability of backup capabilities to support national security operations.

9.9 Cryptographic Security Plan (CSP)

9.9.1. A Cryptographic Security Plan shall be required for all space systems covered by this NPR if they have NSA-approved cryptography as directed in NSTISSP No. 12. Contact the OSPP and/or NASA COR for details related to this requirement.

9.10 Waivers

9.10.1. Waivers to specific policy requirements of this NPR will be considered on a case-by-case basis. Requests shall be sent through the organization’s chain of command and the appropriate DAA’s. Each shall indicate their approval or disapproval of the request. If all approve, the request shall be forwarded to the NASA HQS OSPP; otherwise, it shall be returned to the originator with an explanation for the disapproval. Waiver form can be obtained from Appendix B of this NPR. The NASA HQS OSPP shall request and review any pertinent information involving NSA and IC related issues.

9.10.2. Each organization receiving a waiver request shall provide their operational and technical assessments along with recommendations to the NASA HQS OSPP for consolidation and review.

9.10.3. Each organization shall evaluate requested waivers to this NPR to determine how the waivers, if granted, will result in avoiding unacceptable or adverse impacts on mission, operational plans, and orders; cost or schedule impacts that are determined to be excessive relative to the protection afforded; or any inappropriate or unnecessary protection requirements.

9.11 Roles and Responsibilities

9.11.1. Office of Security and Program Protection (OSPP)

a. Establish within the OSPP a Space Asset Protection entity with sufficient resources (e.g., personnel, budgets, and skills) to carry out the requirements set forth in this NPR.
b. Oversee and manage all threat activities related to NASA-owned or controlled orbital and sub-orbital space systems and platforms programs, particularly those activities involving the Intelligence Community (e.g., CIA, DIA, NRO, and NSA).
c. Perform independent evaluation of IA program performance and resource availability to ensure the implementation of the overall IA program related to NASA-owned or controlled orbital and sub-orbital space systems and platforms.
d. Adjudicate requested waivers to the NASA-unique policy requirements of this NPR.
e. Oversee the assignment of DAA's, CA, and User Representatives, and confidentiality levels to NASA-owned or controlled orbital and sub-orbital space systems and platforms covered by this policy.
f. Provide ISSE support and guidelines to NASA-owned or controlled orbital and sub-orbital space systems and platforms programs beginning with concept and technology development, and continuing throughout their life cycle to assist and help guide protection of NASA program efforts.
g. Oversee and evaluate the implementation, integration, and/or embedment of cryptography into NASA-owned or controlled orbital and sub-orbital space systems and platforms.
h. Provide IA advice and assistance to NASA space-related acquisition and operational components planning to contract for the design, development, manufacture, acquisition, lease, launch, or operation of any space system to be used by NASA.
i. Provide guidance on the use of COTS IA or IA-enabled IT products (i.e., hardware, software, and firmware) being considered for application in NASA-owned or controlled orbital and sub-orbital space systems and platforms.
j. Decide on a discretionary basis, in consultation with the system DAA, whether a space system is past the point of program initiation, but still in development, or a legacy system undergoing major redesign, which shall be subject to the full provisions of this NPR. This decision shall be based primarily on whether the potential IA-related risks of non-compliance outweigh the cost and schedule impact of complying with this NPR.

k. Provide oversight of all IA activities related to NASA-owned or controlled orbital and sub-orbital space systems and platforms within the scope of this NPR.

l. Serve as the principal advisor to the NASA CIO and Program Managers on IA matters for NASA-owned or controlled orbital and sub-orbital space systems and platforms that are outside the scope of this NPR.

9.11.2. Program/Project Managers

a. Ensure compliance with the IA requirements of this policy for developing, acquiring, deploying, leasing, operating, and maintaining all NASA-owned or controlled orbital and sub-orbital space systems and platforms that are used by NASA to collect, generate, process, store, display, transmit, or receive national security and DoD sensitive information, or that perform national security functions throughout their life cycle.
b. Incorporate IA products, services, measures, and techniques throughout the life cycle of all information systems (IS's) and networks that are integral to or essential for the operation of all NASA-owned or controlled orbital and sub-orbital space systems and platforms.
c. Ensure there are duly appointed DAA's for NASA-owned or controlled orbital and sub-orbital space systems and platforms, including those that are at or beyond the point of program initiation.
d. Plan, program, budget for, implement, and manage programs for the development, production, acquisition, integration, maintenance, disposal, and/or life cycle support of IA products or operational measures into space systems used by NASA for which they are responsible.
e. Ensure, through contractual or formal agreements, that the requirements of this policy are applied to all NASA contracts and commercial, involved in the deployment, operation, or maintenance of orbital and sub-orbital space systems and platforms used by NASA. Solicitations, contracts, or formal agreements shall include specific requirements for IA products, reviews, evaluations, services, measures, or techniques, as required by this NPR and mission requirements. Coordinate with the NASA HQS OSPP to get guidance, advice, and current information to assist with developing appropriate IA-related language for such solicitations, contracts, or formal agreements.
f. Ensure COTS IA or IA-enabled IT products being considered for use on NASA-owned or controlled orbital and sub-orbital space systems and platforms for ensuring total system integrity are limited to products evaluated and approved by the policy set forth in NSTISSP No. 11.
g. Ensure continuity of operations planning and procedures account for the availability of backup capabilities to support NASA system operations, in the event affected systems are unable to be restored along timelines needed to reconstitute and assure mission support.
h. Ensure Program/Project Managers for space systems under their purview include performing ISSE and C&A in their program plans, budgets, and contracts, as appropriate.

i. Coordinate on waiver requests related to this NPR.

j. Ensure space systems are included within the IS incident reporting program as a component of NASA-wide incident reporting set forth in this NPR.

k. Develop defensive actions necessary to deter or defeat unauthorized activity (e.g., computer network attack and computer network exploitation against NASA-owned or controlled orbital and sub-orbital space systems and platforms and minimize damage from such activities).

9.11.3. Procurement

a. Ensure, through contractual or formal agreements, that the requirements of this policy are applied to all NASA contracts involved in the deployment, operation, or maintenance of national security space systems or platforms used by NASA. Solicitations, contracts, or formal agreements shall include specific requirements for IA products, reviews, evaluations, services, measures, or techniques, as required by this NPR and mission requirements. Coordinate with the NASA HQS OSPP to get guidance, advice, and current information to assist with developing appropriate IA-related language for such solicitations, contracts, or formal agreements.

CHAPTER 10: Wireless Devices, Services, and Technologies

10.1 General

10.1.1. This chapter establishes policy and assigns responsibilities for the use of wireless devices, services, and technologies in NASA. Hereafter, the term "wireless" means wireless devices, services, and technologies. It directs the development and use of a wireless Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Agency as it relates to classified national security information (CNSI). It also promotes joint interoperability using standards throughout NASA for wireless services, devices, and technological implementations, which may have impact to national security.

10.1.2. This NPR applies to all NASA personnel, contractors, and visitors that enter NASA facilities or that have access to NASA information. It applies to all commercial wireless devices, services, and technologies, including voice, data, and video capabilities, that operate either as part of NASA Information Technology (IT) infrastructure, or as part of NASA stand-alone systems. This includes, but is not limited to: commercial wireless networks, Personal Digital Assistants (PDA), and Portable Electronic Devices (PED). A PDA is a generic term for a class of small, easily carried electronic devices used to store and retrieve information. A PED is any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDA's, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

10.1.3. This Chapter does not apply to Information Systems (IS) and/or Sensitive Compartmented Information Facilities (SCIF) to which Director of Central Intelligence Directive (DCID) 6/9 and DCID 6/3 apply; i.e., Sensitive Compartmented Information (SCI) and special access programs for intelligence under the purview of the Director of National Intelligence.

10.1.4. This chapter of the NPR does not apply to receive-only pagers, Global Positioning System (GPS) receivers, hearing aids, pacemakers, other implanted medical devices, or personal life support systems.

10.2 Wireless Technologies

10.2.1. Wireless technologies enable one or more devices to communicate without physical connections – without requiring network cabling. Wireless technologies range from simple devices such as wireless headphones, microphones, and other devices that do not process or store information to complex systems, such as cell phones and wireless local area networks (WLAN's). They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse.

10.2.2. A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. The most commonly used wireless handheld devices such as text-messaging devices, PDA's, and Smart Phones. Other devices include wireless e-mail devices with push technology, whereby e-mail gets delivered to the device without the user actually polling a Server (e.g., RIM's Blackberry device).

10.3 Wireless Policy

10.3.1. Wireless devices, services, and technologies that are integrated or connected to NASA networks are considered part of those networks, and shall comply with NASA NPD 2810.C and shall be certified and accredited in accordance with their respective national and NASA polices and procedures for unclassified and classified information.

10.3.2. Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit written approval of the cognizant DAA. If approved by the DAA, only assured channels employing National Security Agency (NSA)-approved encryption shall be used to transmit classified information. Classified data stored on PED's shall be encrypted using NSA-approved encryption consistent with storage and treatment of classified information.

10.3.3. Measures shall be taken to mitigate denial of service attacks. These measures shall address not only external threats, but potential interference from friendly sources.

10.3.4. Introduction of wireless technologies in NASA IS's, including those creating an external interface to non-NASA systems [or allowing use of NASA wireless devices that may have impact on non-NASA networks (e.g., SIPRNet and JWICS)] can have a significant adverse effect on the security posture of the IS and requires security review and documentation in the applicable SSAA/SSP.

10.3.5. During the wireless planning stage and prior to acquisition, all NASA wireless projects shall undergo a review by the local chief of security and a duly appointed NASA Certified TEMPEST Technical Authority (CTTA) to determine the potential impact to national security. Results of the analysis shall be documented, protected to their appropriate classification level, and placed in the applicable SSAA/SSP's.

10.3.6. Cellular/PCS and/or other RF or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA).

10.3.7. Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the

CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

10.3.8. DAA's shall ensure that Wireless Personal Area Network (WPAN) capability is removed or physically disabled from a device that processes national security information. Exceptions may be granted on a case-by-case basis as determined by the DAA and shall be documented in the SSAA/SSP.

10.3.9. NASA shall actively screen for wireless devices, which may impact national security information. Active electromagnetic sensing at NASA or contractor premises to detect/prevent unauthorized access of NASA IS's may be periodically performed by the cognizant DAA or CA to ensure compliance with this NPR.

10.3.10. Downloading of mobile code shall only be allowed from trusted sources over assured channels for wireless technologies, which involve national security information.

10.3.11. A NASA wireless KM process shall be established. The goal is increased sharing of NASA wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.

a. The KM process shall be utilized by DAA's to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.
b. DAA's shall submit alternative mitigating techniques for inclusion in a KM database. NASA shall use the wireless KM process to coordinate, prioritize, and avoid duplication of vulnerability assessments of wireless devices.
c. Information on vulnerability assessments shall be considered for classification in accordance national and NASA classification guidance.

10.3.12. NASA national security DAA's system CA's shall:

a. Control wireless access to IS's under their cognizance to ensure that the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems.
b. Include intrusion detection methodologies for wireless systems.
c. Incorporate wireless topics into annual IA training.
d. Review risk assessment results to make an informed and affirmative decision about the risk before granting an exception to this policy.
e. Ensure wireless devices, services, and technologies are considered as an integral aspect of the threat, risk, and vulnerability assessments, which shall be documented in the SSAA/SSP.

Appendix A

Space Systems Security Plan (SSSP)
Orbital and Sub-orbital Platforms

The SSSP is a living document that reflects the formal agreement among the DAA, the certifier, the user representative, and the program manager. The SSSP is developed in the very early stages of system planning and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSSP should contain the information in the following format for *collateral* national security systems. **Note: Systems that process *SCI* or *SAP* information shall be in compliance with DCID 6/3.**

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
1.1 System Name and Identification
1.2 System Description
1.3 Functional Description
1.3.1 System Capabilities
1.3.2 System Criticality
1.3.3 Classification and Sensitivity of Data Processed
1.3.4 System User Description and Clearance Levels
1.3.5 Life Cycle of the System
1.4 System Concept of Operations (CONOPS) summary
2.0 ENVIRONMENT DESCRIPTION
2.1 Operating environment
2.1.1 Facility Description
2.1.2 Physical Security
2.1.3 Administrative Issues
2.1.4 Personnel
2.1.5 COMSEC
2.1.6 TEMPEST
2.1.7 Maintenance Procedures
2.1.8 Training Plans
2.2 Software Development and Maintenance Environment
2.3 Threat Description
3.0 SYSTEM ARCHITECTURAL DESCRIPTION
3.1 System Description
3.2 System Interfaces and External Connections
3.3 Data Flow
3.4 Accreditation Boundary
4.0 SYSTEM SECURITY REQUIREMENTS
4.1 National and Organizational Security Requirements
4.2 Governing Security Requisites
4.3 Data Security Requirements
4.4 Security CONOPS
4.5 Network Connection Rules
4.6 Configuration and Change Management Requirements
4.7 Re-accreditation Requirements
5.0 ORGANIZATIONS AND RESOURCES

5.1 Organizations
5.2 Resources
5.3 Training
5.4 Other Supporting Organizations
6.0 NIACAP WORK PLAN
6.1 Tailoring Factors
6.1.1 Programmatic Considerations
6.1.2 Security Environment
6.1.3 IT System Characteristics
6.1.4 Reuse of Previously Approved Solutions
6.2 Tasks and Milestones
6.3 Schedule Summary
6.4 Level of Effort
6.5 Roles and Responsibilities

Appendices should be added to include system C&A documents; optional appendices may be added to meet specific needs. All documentation relevant to the systems' C&A should be included in the SSSP.

APPENDIXA. Acronym list
APPENDIXB. Definitions
APPENDIXC. References
APPENDIXD. Security Requirements and/or Requirements Traceability Matrix
APPENDIXE. Security Test and Evaluation Plan and Procedures
APPENDIXF. Certification Results
APPENDIXG. Risk Assessment Results
APPENDIXH. Certifier's Recommendation
APPENDIXI. System Security Policy
APPENDIXJ. System Rules of Behavior
APPENDIXK. Security Operating Procedures
APPENDIXL. Contingency Plan(s)
APPENDIXM. Security Awareness and Training Plan
APPENDIXN. Personnel Controls and Technical Security Controls
APPENDIXO. Incident Response Plan
APPENDIXP. Memorandums of Agreement – System Interconnect Agreements
APPENDIX Q. Applicable System Development Artifacts or System Documentation
APPENDIXR. Accreditation Documentation and Accreditation Statement

Note: Systems that process *SCI* or *SAP* information shall be in compliance with DCID 6/3.

Appendix B

FORMAT FOR REQUESTING WAIVERS

(Organization's Letterhead)

DATE:

MEMORANDUM FOR: NASA HQS, Office of Security and Program Protection, Attention: Assistant Administrator, 300 E. St, SW, Washington, DC, 20546

THRU:

Chain of Command, Address, City, State, Zip Code

Approve________Disapprove________

Designated Approving Authority, Address, City, State, Zip Code

Approve________Disapprove________

SUBJECT: Waiver to NPR 16XXX[date], National Security Systems

1. Request an exception to paragraph x.x.x.

2. Explanatory details: *(Briefly describe pertinent system or mission requirements, capabilities and information assurance concerns, and their relation to waiver.)*

3. Justification for exception: (The justification shall include acknowledgement that the *organization has assessed the threats, vulnerabilities, and overall risk associated with the waiver.)*

4. Impact if waiver is not granted: (Provide a succinct impact statement describing the impact *on operations if the wavier is not granted.)*

5. Point of Contact for Waiver:

Signature Block

Waiver requests may be mailed, faxed, or emailed through channels appropriate for the classification level. Contact the intended recipients for current fax numbers or email addresses.